СЕКЦІЯ 5
БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

Дячков Д. В., канд. екон. наук, доцент,
Полтавська державна аграрна академія

МОДЕЛЬ ФОРМУВАННЯ СТРАТЕГІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

В умовах глобалізації та інформатизації соціально-економічних відносин процеси забезпечення безпеки перетворюються в один з найважливіших елементів підтримки бізнесу. Проте увага фахівців у сфері інформаційної безпеки, IT-безпеки та кібербезпеки переважно спрямована на формування політики інформаційної безпеки, визначення рівня інформаційної безпеки, заходів відвернення кібератак, використання новітніх технічних засобів та впровадження програмних продуктів з метою захисту інформації. Водночас питання формування та реалізації стратегії інформаційної безпеки залишається поза увагою як науковців, так і практиків у сфері інформаційного захисту. У багатьох організаціях існує реальна необхідність розробки окремих незалежних від IT-стратегій, стратегій управління інформаційною безпекою, які могли б, поряд з необхідним рівнем захисту, забезпечити належну підтримку бізнес-процесів підприємств та їх ефективний розвиток.

Наразі найбільш розповсюдженим є підхід до визначення стратегії інформаційної безпеки, який базується на побудові матриці на основі двох критеріїв. Перший критерій класифікації передбачає, що процеси захисту інформації дуже залежить від значної кількості випадкових і важкопередбачуваних факторів, зокрема поведінки зловмисника, впливу природних явищ, збоїв і помилок у процесі функціонування елементів системи обробки інформації тощо. Другий критерій класифікації визначає, що серед засобів захисту значне місце займають організаційні заходи, пов’язані з дією персоналу.

Обґрунтування змісту необхідних стратегій у межах розглянутого підходу здійснюється за двома критеріями: визначення необхідного рівня захисту та ступеню свободи дій у процесі організації захисту. Значення першого, формалізується безліччю загроз, щодо яких має бути забезпечений захист: 1) від найбільш небезпечних із вже відомих загроз; 2) від усіх відомих загроз; 3) від усіх потенційно можливих загроз. Другий критерій вибору стратегій захисту зводиться до того, що організатори і виконавці процесів захисту мають відносно повну свободу розпорядження методами і засобами захисту і деякий ступінь свободи втручання в архітектурну побудову системи обробки інформації, а також в організацію і забезпечення технології її функціонування. Відповідно виділяють три основні ступені свободи: 1) будь-яке втручання в систему обробки інформації не допускається. Таку вимогу може бути встановлено до вже функціонуючих систем обробки інформації, а порушення процесу їх функціонування для установки механізмів захисту не дозволяється; 2) до архітектурної побудови системи обробки інформації та технології її функціонування допускається пред’являти вимоги не концептуального характеру. Тобто допускається припинення процесу функціонування системи обробки інформації для встановлення деяких механізмів захисту; 3) вимоги будь-якого рівня, зумовлені потребами захисту інформації, вважаються обов’язковии під час побудови системи обробки інформації, організації та забезпеченні їх функціонування [1].

Відповідно можна виділити три основні стратегії, представлені в табл. 1.

Таблиця 1 – Стратегії захисту інформації [1]

Загрози, що враховуються	Вплив на системи обробки інформації		
	Відсутній	Частковий	Повний
Найбільш небезпечні	Захисна стратегія		
Всі відомі		Наступальна стратегія	
Всі потенційно можливі			Попереджувальна стратегія

Проте динамічність інформаційного середовища, формування глобального інформаційного простору, міжнародна взаємодія у сфері інформаційно-комунікаційних технологій висувають на першочерговий план формування більш адаптивної моделі визначення стратегії інформаційної безпеки, яка б враховувала найрізноманітніші фактори впливу на як виробничі та управлінські бізнес-процеси, так і на інформаційну систему підприємства, а також охоплювала цілі загальної стратегії підприємства. З цією метою пропонується модель визначення стратегії інформаційної безпеки підприємства, яка б відповідала вищезазначеним вимогам (рис. 1).

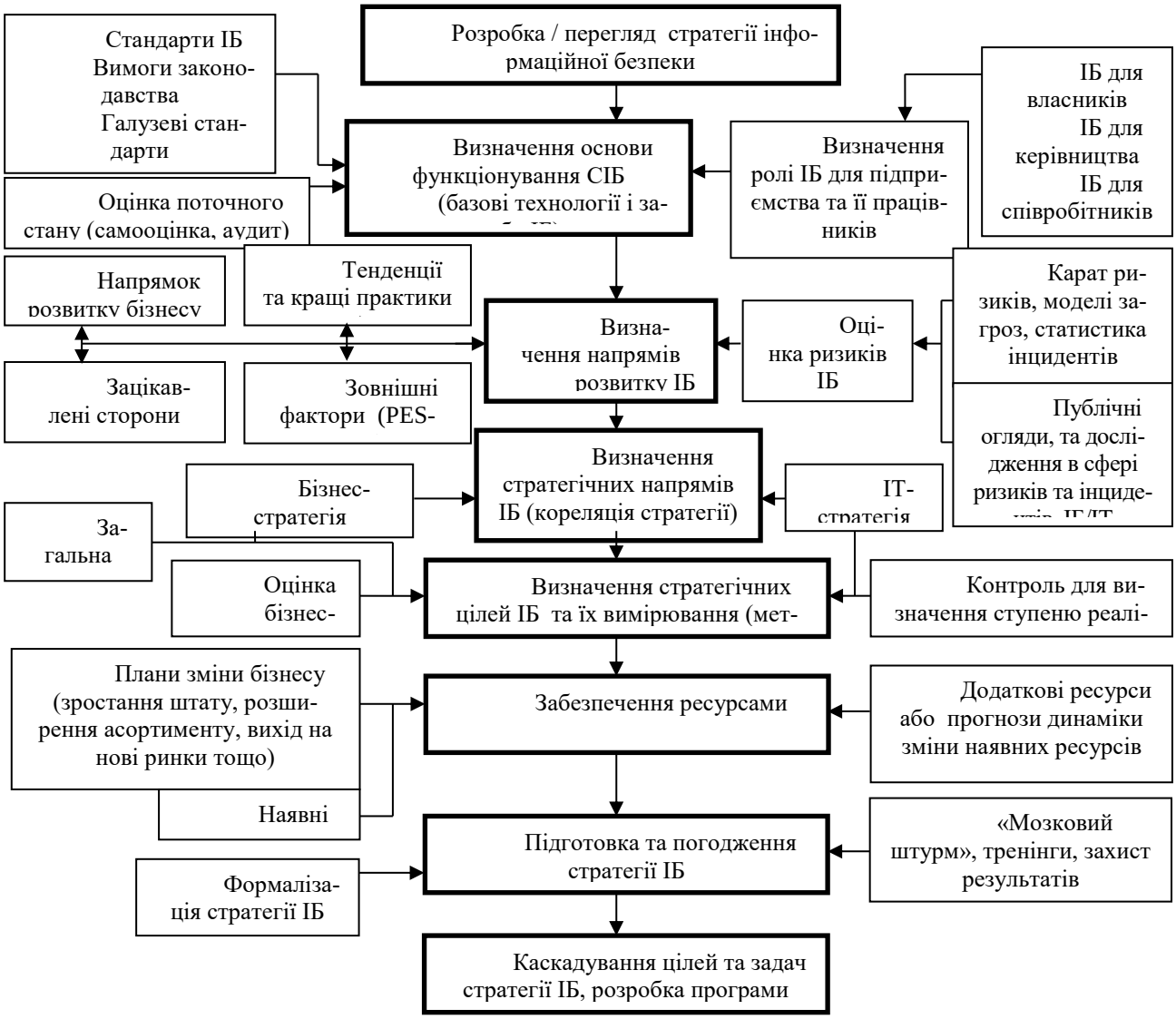

Рисунок 1 – Пропонована модель визначення стратегії інформаційної безпеки підприємства [розроблено на основі 2]

В основі комплексу заходів щодо захисту інформації повинна бути стратегія інформаційної безпеки, яка б визначала цілі, критерії, принципи і процедури, необхідні для побудови надійної системи захисту. В умовах всеохоплюючої інформатизації, стратегія захисту інформації в найзагальнішому вигляді може бути визначена як пошук оптимального компромісу між потребами в захисті і необхідними для цих цілей ресурсами.

Список використаних джерел:

1. Стратегии защиты информации. URL: https://studfiles.net/preview/1770970/page:15/
2. Стратегия информационной безопасности. URL: http://docplayer.ru/43503819-Strategiya-informacionnoy-bezopasnosti.html

Кирилишен Я. В., канд. екон. наук, доцент,
Донецький національний університет імені Василя Стуса, м. Вінниця

ВИКОРИСТАННЯ МЕТОДУ MOBILE-FIRST ДЛЯ РОЗРОБКИ САЙТІВ

За даними сайту statista.com доля трафіку мобільних пристроїв складає 52,2 %. В Азії цей показних складає 65,1 % від всього інтернет трафіку. Дані рис. 1 свідчать про стрімкий ріст популярності та збільшення долі інтернет трафіку мобільних пристроїв у світі. У 2009 році частка мобільних девайсів складала лише 0,7 %, але з кожним роком та появою нових технологій вона збільшувалася.

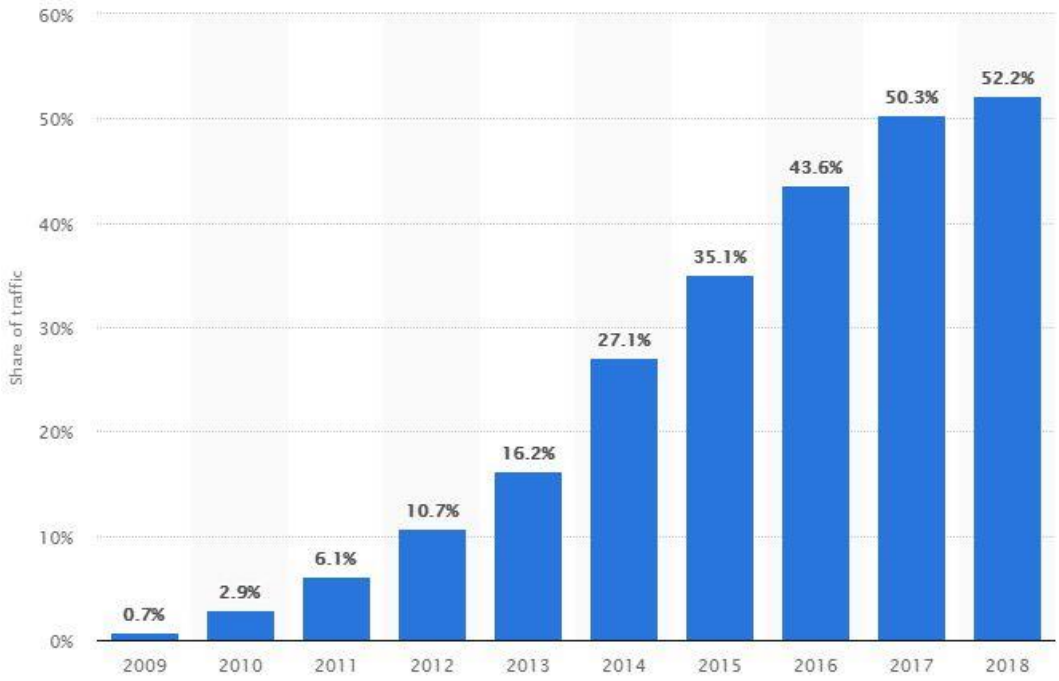

Рисунок 1 – Доля інтернет трафіку мобільних пристроїв у світі

Тому мобільний трафік стає більш значущим і власники веб-сайтів повинні зважати на цю статистику. Як показує практика, користувачі мобільних телефонів і планшетів проводять